

AO 106 (Rev. 5/85) Affidavit for Search W.

United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person or property to be searched)

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

[REDACTED]
Dover, Delaware 19901,
described more particularly
on Attachment A

SEALED

CASE NUMBER: 08-20-M

I, David B. Yearly, being duly sworn depose and say:

I am a(n) U.S. Immigration and Customs Enforcement Agent and have reason to believe
Official Title

that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

in the _____ District of Delaware
there is now concealed a certain person or property, namely (describe the person or property)
described in Attachment B

which is (give alleged grounds for search and seizure under Rule 41(b) of the Federal Rules of Criminal Procedure)
evidence of a crime and contraband

in violation of Title 18 United States Code, Section(s) 2252 and 2252A
The facts to support the issuance of a Search Warrant are as follows:

Affidavit attached.

Continued on the attached sheet and made a part hereof.

☒ Yes ☐ No

Sworn to before me, and subscribed in my presence

Date

February 5, 2008

at

Wilmington, Delaware
City and State

Honorable Leonard P. Stark
United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Affiant
David B. Yearly, Special Agent
U.S. Immigration & Customs Enforcement

Signature of Judicial Officer

ATTACHMENT A:

DESCRIPTION OF LOCATION TO BE SEARCHED

The residence located at:

[REDACTED]
Dover, Delaware 19901

[REDACTED] is an end unit three-story town home. The numbers '[REDACTED]' are located on a post on the left hand side of the front door of the residence, this post supports a small roof over the front door. The front of the residence has two windows in the basement, a bay window on the 1st floor with a red front door, the 2nd floor has three windows with red shutters and the roof has on the front of the residence. On the side of the house the 1st floor has one bay window and one small window with red shutters, the 2nd floor has two windows with red shutters. The roof has two dormers facing the front of the house on [REDACTED]. The back of the town house has a back door that opens onto a wooden deck with steps leading to the ground. The exterior of the Town House is tan vinyl siding, with the basement exterior being concrete on the side and brick in the front.

ATTACHMENT B:

DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED

The following is a description of the items evidencing violations of Title 18, United States Code, Sections 2252 and 2252A to be searched for and seized, pursuant to the attached search warrant. The seizure and search of computers and computer media will be conducted in accordance with the process described in the affidavit submitted in support of this warrant:

a. images of child pornography, files containing images of child pornography in any form, and records or materials relating to such images, including the images discussed in this affidavit,

wherever they may be stored or found, including, but not limited to:

- i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer-related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), any electronic data storage devices (including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums), any input/output peripheral devices (including but not limited to passwords, data security devices and related documentation), and any

hardware/software manuals related to or used to visually depict child pornography, to contain information pertaining to the interest in child pornography; and/or to distribute, receive, or possess child pornography, as well as information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and


ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the

transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

- c. credit card information, including but not limited to bills and payment records, such as records relating to the purchases discussed in this affidavit;
- d. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and
- e. records or other items which evidence ownership or use of computer equipment or activity found in the above residence, including, but not limited to, sales receipts, bills or records regarding procurement of Internet access, records regarding accounts held with ISPs and handwritten notes.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH)
OF THE RESIDENCE LOCATED AT:)


Dover, Delaware 19901

)
) Case No. 08-

)
) FILED UNDER SEAL
)
)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David B. Yeary, being duly sworn, depose and state the following:

1. I am a Special Agent with United States Immigration and Customs Enforcement ("ICE"), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of search warrants. I have been employed as a Special Agent for ICE for approximately five years and am currently assigned to the Resident Agent in Charge Office in Wilmington, Delaware. My responsibilities include conducting investigations into various types of federal crimes, including crimes involving child pornography. I have received training from ICE regarding child pornography, the sexual abuse of children, the behavior of preferential child molesters and how to conduct investigations of child sexual exploitation and obscenity crimes. As part of my work on these cases and in these training courses, I have observed and reviewed numerous examples of child pornography (as that term is defined in 18 U.S.C. § 2256) in all forms of media, including computer media. In the course of my investigative duties, I have also had contact, in the form of interviews and meetings, with preferential child pornographers and those involved in the

distribution, sale, and possession of child pornography. And I have assisted in the execution of numerous search warrants relating to investigations of child pornography crimes.

2. This affidavit is submitted in support of an application for a search warrant for the residence of Jonathon AMATO, located at [REDACTED], Dover, Delaware 19901 (the "Subject Premises") and the computer(s) located therein, for evidence of violations of Title 18, United States Code, Sections 2252 and 2252A ("Section 2252" and "Section 2252A"). The Subject Premises is more fully described in Attachment A.

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Section 2252 and Section 2252A is presently located at the Subject Premises.

RELEVANT STATUTES

4. This investigation concerns alleged violations of Section 2252 and Section 2252A, relating to material involving the sexual exploitation of minors.

5. Sections 2252 and 2252A prohibit a person from, *inter alia*, knowingly transporting, receiving, or distributing child pornography in interstate or foreign commerce, by any means including by computer, or from possessing child pornography that has been transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

7. "Child pornography" means any visual depiction of sexually explicit conduct where (a) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

8. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

9. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

10. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

11. "Internet Service Providers" ("ISPs") are commercial organizations which provide individual and business customers a range of capabilities, such as access to the Internet and access to other functions including web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs offer customers various means by which they can access the Internet, such as (a) through the use of a "dial-up" system whereby the customer accesses the

Internet via a telephone line; (b) broadband-based access, whereby a customer accesses the Internet via a digital subscriber line ("DSL") or cable television line; (c) access to the Internet via dedicated circuits; or (d) a satellite-based subscription that provides Internet access. ISPs typically charge the customer a fee based upon the type of connection the customer chooses to employ and the volume of data (or "bandwidth"), that the connection supports. Many ISPs assign each subscriber an account name (often referred to as a "user name" or "screen name"), an e-mail address and an e-mail mailbox. The subscriber, in turn, typically creates a password that allows for restricted access to the account. Therefore, by using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can then access the Internet by inputting his or her account name and password.

12. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address ("IP address"). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first-level, or top-level domains are typically: (a) ".com" for commercial organizations; (b) ".gov" for governmental organizations; (c) ".org" for organizations; and (d) ".edu" for educational organizations. Second-level domains will further identify the organization, as, for example, "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each domain is uniquely identifiable. For example, "www.usdoj.gov" identifies the world wide web server located at the United States Department of Justice, which is

part of the United States government.

13. "Log Files" or "logs" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events, including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

14. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

15. A "website" consists of textual pages of information (called "web pages") and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Markup Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

16. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains (a) the name of the protocol to be used to access the file resource; (b) a domain name that identifies a specific computer on the Internet and (c) a "pathname," which is a hierarchical description that specifies the location of a file in that computer.

17. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND REGARDING SEIZURE OF COMPUTERS

18. Based upon my knowledge, training and experience, as well as the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most or all of the items that relate to that computer (including hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

19. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it

is included in the search warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

20. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and software available today requires that even computer experts must specialize in some systems and applications. Before a search is conducted, it is difficult to know which expert should analyze the computer system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

21. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the computer monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices, to understand how that data was created. Moreover, searching computerized information for evidence or instrumentalities of a crime commonly requires the seizure of the

entire computer's input/output peripheral devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system.

22. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that not only the computer, but also its storage devices, the monitor, keyboard, printer, modem and the other system components were all used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

BACKGROUND REGARDING THE INTERNET

23. As previously noted, your affiant has received formal training in the investigation of crimes involving child pornography and the sexual exploitation of children. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

24. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from an ISP, which connects them to the Internet. In doing so, the ISP assigns each device that accesses the internet an IP address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same

way every telephone has a unique telephone number. An IP address is composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. Each time a device accesses the Internet, the device from which initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ "dynamic" IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address. It can identify the user of that IP address for a particular computer session from these records, so long as the ISP has retained the records dating back to that time period.

25. Photographs and other images can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner," which is an optical device that can recognize characters on paper and, by using specialized software, convert them to digital form. Images can also be captured from single frames of video on a computer. After the photograph or other image has been scanned into or captured by the computer, the computer can store the data from the image as an individual "file." Such a file is known as an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

26. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A compact disk can store hundreds of images and thousand of pages of

text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage on a different computer system in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

27. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laserjet or inkjet printer).

28. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. This can occur in various ways. For example, electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants

of deleted files, may reside in “free space” or “slack space” – that is, in space on the hard drive that is not allocated to an active file or that is left unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION

29. In April 2006, Immigration and Customs Enforcement’s Cyber Crimes Center, Child Exploitation Section (“ICE/C3/CES”) initiated an investigation into a criminal organization operating or controlling numerous commercial child exploitation websites. The investigation began with the identification of one such website known as “Home Collection,” which was located at <http://members.homccollect.us>.

30. As set forth more particularly below, the investigation soon revealed that the organization was operating in excess of 200 commercial child exploitation websites, access to which was restricted to those who paid to become “members” of the sites (“member-restricted websites”). The organization solicited customers to pay for access to these member-restricted websites through the use of a number of “advertising websites.” When a customer visited these advertising

websites, he or she was offered monthly access to a member-restricted website for a fee of between \$79.95 and \$99.95 per month. The organization then utilized various PayPal¹ accounts to process customer payments for access to the member-restricted websites.

31. From April 2006 through August 2007, ICE/C3/CES conducted over 175 undercover transactions at the advertising websites associated with this investigation, which in turn provided access to approximately 40 different member-restricted websites containing child pornography. Each one of the undercover purchases followed one of the two patterns listed below:

Pattern One:

1. The ICE agent accessed a specific advertising website.
2. When the ICE agent clicked on an icon indicating that he or she wished to obtain access to a member-restricted website, the agent was redirected to an "iWest" payment website. That website required that the agent enter personal identifying information, including an e-mail account and credit card information. In addition, the "iWest" payment website identified the specific member-restricted website that the customer was purchasing access to, through the use of a "website identifier" – a name associated with the particular website.
3. After the agent completed the required information and clicked "submit," the agent was redirected to a second web page indicating that the payment was currently being processed. The website also stated that the agent should check the e-mail account the agent had typed into the iWest website and that the agent would receive an e-mail at that address providing further information on how to complete their purchase.
4. The ICE agent next received an e-mail at the e-mail address he or she had typed into the iWest payment website, which contained payment completion instructions. This e-mail

1

According to its website, located at <http://www.PayPal.com>, PayPal is a company that enables any individual or business with an e-mail address to securely, easily and quickly send and receive payments online, using a credit card or bank account information. It is becoming an inexpensive way for merchants to accept credit cards in their on-line storefronts instead of using a traditional payment gateway. PayPal identifies its accounts by the name of the e-mail address(es) that a PayPal account holder provides to PayPal when registering for the account.

included a hyperlink to a PayPal account and it instructed the agent to access that account in order to complete the transaction.

5. The ICE agent completed the transaction by again entering personal identifying information into the PayPal website and ultimately by making a payment to the owner of the PayPal account via credit card transaction. After completing the transaction via the PayPal account, the ICE agent received a receipt from PayPal, which contained an "Item/Product number."
6. The ICE agent then received an e-mail from the organization, which provided the agent with the URL for the member-restricted website the agent had gained access to, as well as password and login information to enable the agent to access the site.

Pattern Two:

7. The ICE agent accessed a specific advertising website.
8. When the ICE agent clicked on an icon indicating that he or she wished to obtain access to a member-restricted website, the agent was redirected to an "iWest" payment website. That website required that the agent enter personal identifying information, including an e-mail account and credit card information. In addition, the "iWest" payment website identified the specific member-restricted website that the customer was purchasing access to, through the use of a "website identifier" – a name associated with the particular website.
9. After the agent completed the required information and clicked "submit," the agent was redirected to a second web page that indicated that the payment was currently being processed. The web page also contained a button the agent had to click to complete the payment.
10. The agent clicked the button and was redirected to a secure PayPal payment web page.
11. The ICE agent completed the transaction by again entering personal identifying information into the PayPal website and ultimately by making a payment to the owner of the PayPal account via credit card transaction. After completing the transaction via the PayPal account, the ICE agent received a receipt from PayPal, which contained an "Item/Product number."

12. The ICE agent then received an e-mail from the organization, which provided the agent with the URL for the member-restricted website the agent had gained access to, as well as password and login information to enable the agent to access the site.

**IDENTIFICATION OF CERTAIN PAYPAL ACCOUNTS AND
CERTAIN MEMBER-RESTRICTED WEBSITES**

32. As indicated above, this criminal organization utilizes multiple PayPal accounts to process customer payments for the monthly subscription fees required to gain access to its child exploitation member-restricted websites. PayPal maintains transactional records for each such PayPal account. During its investigation, ICE/C3/CES obtained the transactional records for the particular PayPal accounts the organization used to facilitate customer payments for access to the member-restricted websites. The transactional records include at least the following items for each such transaction: the date of purchase, the time of purchase, the name of the customer, the subject of purchase, the amount of the purchase, the customer's IP address, the customer's e-mail address, the seller's e-mail address, an "Item ID" number and the customer's full billing address. The subject of the purchase refers to the notation in the "Subject" column in the PayPal transactional records listed below.

33. The PayPal accounts that ICE agents utilized to make the undercover transactions described above are as follows (listed by the business name that accompanied the account, the primary e-mail address that was associated with the account and any alternate e-mail addresses associated with the account):

Business Name	Primary E-mail Address	Alternate E-mail Addresses
Proof Soft	androdork@gmail.com	androdork@yahoo.com

		bsbsoft8@yahoo.com
Lencomps LTD	zakiyyah777@yahoo.com	lencomps@juno.com
Proof Soft	a_chakin@yahoo.com	
Belfast LTD	belfastltd@juno.com	caly@phoenixorder.com emhigh@charter.net
Belfast LTD	lag89@nc.rr.com	belfast-limited@juno.com
Financial Services	belfast_ltd@juno.com	MMcCary3401@charter.net Financialservice@charter.net
Proof Soft	pallone21@gmail.com	softprf@yahoo.com
Bullet Proof Soft	rrpay@hotmail.com	freewash130@yahoo.com bklmchicano@yahoo.com
Bullet Proof Soft	PReyes1101@hotmail.com	bs_soft66@yahoo.com bsofteawh@yahoo.com phillip_reyes2001@yahoo.com
Bullet Proof Soft	mr.corax@gmail.com	venusdemil023@aol.com freeawh@yahoo.com
Bullet Proof Soft	bsb22flash@yahoo.com	oldervera@gmail.com
Lencomps LTD	itstime2change@hotmail.com	lencompsltd@juno.com
Jfire Financial	jufire@yahoo.com	a_service@freeawh.com a_service@yahoo.com jufire@hotmail.com jufire@collegeclub.com a_soft_tm@yahoo.com
S_Market	webfs@email.com	al_softm@yahoo.com al_soft_tm@yahoo.com
CS S'ven Enterprise	belfast_limited@juno.com	Carlos_Sumpter@charter.net

34. As discussed in paragraph 31, ICE agents have conducted over 175 undercover

transactions during the course of this investigation. The undercover transactions have identified a group of PayPal accounts that are being used to facilitate customer payments to specific child exploitation member-restricted websites. Those specific member-restricted websites could be identified in the PayPal transactional records by looking to the description in the “Subject” column – the name associated with the particular child pornography website that the customer was purchasing access to. The names in this Subject column – referencing particular member-restricted websites – matched the names of the “website identifiers” that ICE agents received after they had entered their personal identifying information into the iWest payment system, during the instances in their investigation when the agents paid to access the member-restricted websites.

In addition to description in the Subject column, for each specific member-restricted website, the criminal organization assigned a unique Item ID number. These Item ID numbers also appeared in the PayPal transactional records. Those Item ID numbers corresponding to particular member-restricted websites matched the “Item/Product Numbers” contained in the receipt that ICE agents received from PayPal, after those agents had paid to access the member-restricted websites during their investigation.

Toward the end of November 2006, the criminal organization stopped using the listed descriptions in the Subject column to identify the specific member-restricted websites that were associated with each purchase. Therefore, for customer purchases before that point in November 2006, PayPal transactional records included both a description in the Subject column listing the particular member-restricted website that a customer was paying to access, as well as an Item ID

number corresponding to that same website. For purchases after this point in November 2006, only the Item ID number associated with the member-restricted website will be present in the PayPal transactional records. The following descriptions were either extracted from the Subject column from the PayPal transactional records or from the website identifier provided to ICE agents on the iWcst payment system. They were then matched with the Item ID number that was associated with that same website during the ICE undercover transactions:

Subject Description	Item ID Number
Home Collection 1000/Sexy Angels	1000
Home Collection 1001/Desired Angels	1001
Home Collection 1002	1002
SickCR Package v5.06 Build 3638	1003
DarkRO XP Tools v2.04	1004
Underage Home	1005
Angel Collection 1006/Lolita Play	1006
Angel Collection 1007	1007
Angel Collection 1010	1010
HL Package/Hardlovers	1012
RH Collection	1013
FD2 Collections	1014
GOL-2 Collections	1016
EXTRA Collections	1017
LOH Collections	1018

LOPAR Collections	1019
NYMST Collections	1020
Secret Collections	1021
Lo Editions 3/4 Collections	1026
BD Hot Collections	1029
BD-Photo Collections	1030
Lust Collections	1034
Red Vids 1	1035
Red Vids 2	1036
Secret Content 2	1037
Shadow Com	1038
Charming	1047
Gentle Angels	1049
Video Nymphets	1121
Lo Video-2 Collections	1126
Pretty X-2 Collections	1128
Under Info-2 Collections	1129
Lo Editions 7/8 Collections	1132
BDM 1-4 Collections	1135
Phang Collections	1138
Spycam Lolitas	1144
Boys Say Go	1156
LS Pics v1.0	1158

Video Shop CD1	1159
Video Shop CD2	1160
Video Shop CD3	1161
Video Shop CD4	1162
Video Shop CD5	1163
Kidz Index	1177
Kinder Schutz Web	1183
Lolitas Mixed	1193
CP City	1202
Extreme Material	1215
Excited Angles	1218
CP Home Video	1222
Pedoland-Kidz Porn	1224
Kidz Index	1227

THE SUBJECT OF THIS SEARCH WARRANT

35. Analysis of the transactional records obtained from PayPal provided the name and billing address of various customers that purchased access to at least one of the identified child pornography member-restricted websites, including the subject of this search warrant, Jonathon AMATO.

36. On January 03, 2007, Jonathon AMATO made a payment to PayPal account Financial Services. The payment was for RH Collection, in the amount of \$94.95. The PayPal

transactional logs provided the following relevant information:

Date: January 03, 2007
Time: 13:27:55 PST
Name: Jonathon AMATO
Subject: Invoice # 30598
Other IP: 71.200.27.10
Gross: \$94.95
From Email Address: [REDACTED]
To Email Address: BELFAST_LTD@JUNO.COM
Item ID: 1013
Referral URL:
<http://www.2007realhard.com/join/index.php?action=finish&ID=30598&key=235ccbb5fb07b5503ed9afd>
First Name: Jonathon
Last Name: AMATO
Primary Email: [REDACTED]
Primary Address: [REDACTED]
Night Phone: [REDACTED]
Signup Date: November 09, 2003
Last Web Access: February 03, 2007

On December 22, 2006, Jonathon AMATO made a payment to PayPal account Financial Services. The payment was for RH Collection, in the amount of \$94.95. The PayPal transactional logs provided the following relevant information:

Date: December 22, 2006
Time: 6:04:43 PST
Name: Jonathon AMATO
Subject: Invoice # 25941
LAST LOGIN IP: 71.200.27.10
Gross: \$94.95
From Email Address: [REDACTED]
To Email Address: belfastltd@juno.com
Item ID: 1013
Referral URL:
<http://pedoland.biz/signup/index.php?action=finish&id=25941&key=7ac035ca0e9ca6029c2e2d36d9fa7285>
First Name: Jonathon
Last Name: AMATO
Primary Email: [REDACTED]

Primary Address: [REDACTED]
Night Phone: [REDACTED]
Signup Date: November 09, 2003
Last Web Access: February 03, 2007

On September 18, 2006, Jonathon AMATO made a payment to PayPal account Financial Services. The payment was for Home Collection 1000, in the amount of \$79.95. The PayPal transactional logs provided the following relevant information:

Date: September 18, 2006
Time: 17:16:32 PST
Name: Jonathon AMATO
LAST LOGIN IP: 71.200.27.10
Gross: \$79.95
From Email Address: [REDACTED]
To Email Address: lencomps@juno.com
Item ID: 1000
Referral URL: None
First Name: Jonathon
Last Name: AMATO
Primary Email: [REDACTED]
Primary Address: [REDACTED]
[REDACTED]
Night Phone: [REDACTED]
Signup Date: November 09, 2003
Last Web Access: February 03, 2007

37. As stated in paragraph 34, ICE agents have conducted over 175 undercover transactions during the course of this investigation. In conducting these undercover transactions, ICE agents have identified specific subject identifiers and Item Ids that are associated with child exploitation member restricted websites. The subject identifier RH Collection refers to a child exploitation member restricted website known as "Real Hard II." ICE agents purchased access to this member restricted website on the following dates: 11/8/06; 12/1/06; 12/12/06; 12/12/06; and on 01/19/07. On each occasion, the transaction was either identified by the subject identifier RH

Collection or the Item ID 1013. The subject identifier Home Collection 1000 refers to a child exploitation member restricted website known as "Sexy Angels." ICE agents purchased access to this member restricted website on the following dates: 8/29/06 and 10/05/06. On each occasion, the transaction was either identified by the subject identifier Home Collection 1000 or the Item ID 1000.

38. As indicated in paragraph 36, the PayPal transactional logs for Jonathon AMATO contained referring URLs of:

<http://www.2007realhard.com/join/index.php?action=finish&ID=30598&key=235ccb5fb07b5503ed9afd> and

<http://pedoland.biz/signup/index.php?action=finish&id=25941&key=7ac035ea0e9ca6029c2e2d36d9fa7285>.

The referring URL indicates the website the customer was viewing immediately prior to connecting to the PayPal payment page. This information identifies the specific website redirecting a customer to a PayPal payment page. NCMEC was able to verify that the URL listed in this paragraph contained child exploitation images.

39. **Real Hard 2/RH Collection:** The member restricted website associated with the subject identifier Real Hard 2 and RH Collection is known as "Real Hard II." The member restricted website contained the following sections: "Home;" "Updates;" "Hardcore;" "Softcore;" "Video;" "Site Support;" and "Logout." There were numerous galleries contained within the "Hardcore," "Softcore," and "Video" sections. A partial capture of the member restricted website was obtained to include the entire subdirectory "Video." The "Video" subdirectory contained eight video files and the following folders: "Boys;" "Long;" "Preteen Action;" and "Small."

There were a total of 44 video files in the "Video" subdirectory. The video files depicted prepubescent female minors engaging in sexually explicit acts. The video files were not submitted to NCMEC. The following descriptions provide a sample of the content in the member restricted website:

Video Hot-Blowjob

(<https://69.50.183.226:10010>) (/Video/Hot-blowjob.mpg)

This video files depicts scenes of a nude prepubescent female minor engaged in oral sex with an adult male. The video starts with the female minor lying between the legs of an adult male on a bed. The female moves to the side of the male continuing oral sex on the adult male. At approx 4:35 minutes the adult male ejaculates into the females mouth. This video is approximately 5:15 in length.

Video Small

(<https://69.50.183.226:10010>) (/Video/Small/II.mpg)

This video files depicts scenes of a nude prepubescent female minor engaged in sexually explicit conduct with an adult male. The video shows a nude female minor on top of an adult male lying on a bed. The adult male is inserting the tip of his penis into the vagina of the female.

40. Home Collection WOO/Sexy Angels: The member restricted website associated with the subject identifiers Home Collection 1000 and "Sexy Angels" is known as "Sexy Angels." The member restricted website contained the following sections: "News;" "Photos;" "Videos;" "Software;" "Message Board;" and "Cancel or Rebill." There were approximately 9,442 images files in the "Photos" section and approximately 186 video files. Several of the images depicted lascivious displays of the female minors' genitalia. The female minors were displayed in sexually suggestive manners. The images were submitted to NCMEC, but NCMEC was unable to match any of the images with known victims. The following image descriptions provide a sample of the content of the

member restricted website:

Image 0096

(<http://sexyangels.freeawh.com/members/photos/old-2004-lolitas-022/image0096>)

This image displays a close up shot of a nude prepubescent female minor's vagina. There are approximately 102 images of the same prepubescent female minor in the listed gallery. The majority of the images depict the female minor at the beach removing her bathing suit. This image focuses on her vagina. The female minor appears to be standing, bent slightly at the waist. The image clearly displays the female minor's anus and vagina.

Image 0059

(<http://sexyangels.freeawh.com/members/photos/ls-magazine-0004/0059.jpg>)

This image displays two nude prepubescent female minors lying on a bed. The closer female minor is lying with her head resting on the other female minor's vagina. They are both lying on their backs. The closer female minor has her left arm behind the left leg of the second female minor and her right hand pointing towards her own vagina. Both of her legs are bent at the knee and her feet are touching. There is a clear display of her vagina and breasts. The second female minor is also lying on her back; her head slight off the bed. Both of her legs are bent at the knee and her feet are also touching. Her legs are raised in the air and each hand is grasping one of her legs at her shin.

Image 0027

(<http://sexyangels.freeawh.com/members/photos/ls-models-0004/0027.jpg>)

This image displays a close up shot of a nude prepubescent female minor's anus and vagina. The female minor has her butt and legs in the air; with her legs spread clearly displaying her anus and vagina.

41. On June 25, 2007, a WHOIS (commercial website identifier) inquiry on IP address 71.200.27.10 was conducted and was found to be issued to a subscriber with Comcast Cable Communications. On July 9, 2007, a subpoena was issued directing Comcast Cable Communications to supply subscriber information as well as Internet connection access logs for the person assigned/using the IP address 71.200.27.10. A response from Comcast Cable Communications was received on July 25, 2007, which indicated that although no information could

be provided relative to the suspect transaction dates listed in paragraph 36 (request past the 180 day retention period of the requested information), the below-listed account subscriber information was confirmed:

Jonathon AMATO
[REDACTED] Dover, Delaware 19901.
Account created 09/28/2006
Account status Active
Email ID [REDACTED]

42. On or about January 28, 2008, representatives of the United States Postal Service informed ICE agents that Jonathon AMATO is currently receiving mail at [REDACTED]
[REDACTED] Dover, Delaware 19901.

43. On February 5, 2008 a response from a subpoena issued to Capital One was received. The subpoena requested information on account number [REDACTED] which was transferred to account number [REDACTED] on August 30, 2007, and on account number [REDACTED]. The billing statement for account number [REDACTED] for the period of 09/16/06 through 10/06/2006 shows a transaction in the amount of \$79.95 charged to Pay Pal *LENCOMPSLTD4029357733CA on 09/19/2006. The billing statement for account number [REDACTED] for the period of 12/18/2006 through 01/04/2007 shows a transaction in the amount of \$94.95 charged to Pay Pal BELFASTLTD4029357733CA on 12/23/2006. The billing statement for account number [REDACTED] for the period of 01/18/2007 through 02/07/2007 shows a transaction in the amount of \$79.95 charged to Pay Pal BULLETPROOF4029357733CA on 02/01/2007.

44. On July 10, 2007, a response from a subpoena issued to America Online Inc. (AOL) was received. AOL records indicate that screen name [REDACTED] [REDACTED] are registered to Jonathon Amato. This account is currently active and was created on 06/16/2001. The address and phone number information that was provided when the account was created is [REDACTED], phone [REDACTED]

45. Surveillance of the [REDACTED] Dover, Delaware 19901, on February 1, 2008, was conducted. A red Chevrolet Corvette bearing Delaware license plate [REDACTED] was parked in front of [REDACTED], Dover, Delaware. A check with the Delaware Department of Motor Vehicles indicated the license plate is assigned to a 2002 Chevrolet Corvette. The owner of record of the 2002 Corvette is Jonathon AMATO, [REDACTED], Dover, Delaware. A check with the Delaware Department of Motor Vehicles also indicated that a 1998 Chevrolet pickup truck is registered to Jonathon AMATO, this vehicle was not present at the address.

46. On or about January 28, 2008, representatives of the United States Air Force Office of Special Investigations (OSI) at Dover AFB confirmed that Jonathon AMATO is an active member of the United States Air Force, stationed at Dover AFB. The following information regarding Jonathon AMATO was confirmed by OSI Special Agent Amber ARMBRUSTER:

AMATO, Jonathan

[REDACTED] Dover, DE 19901

47. Based on my previous investigative experience related to child pornography

investigations, including investigations of subjects who subscribed to websites offering access to child pornography, I have learned that individuals who subscribe to such websites are often individuals who have a sexual interest in children and in images of children, and who download images and videos of child pornography. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials involving children in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their

throughout the world.

CONCLUSION

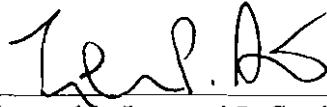
48. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that Jonathan AMATO has engaged in criminal violations of 18 U.S.C. §§ 2252 and 2252A, including the possession and/or receipt of child pornography, and that evidence, fruits, and instrumentalities of criminal violations of 18 U.S.C. §§ 2252 and 2252A may be located at the residence described in Attachment A.

49. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.



David B. Yeary
Special Agent
U.S. Immigration & Customs Enforcement

SUBSCRIBED and SWORN
before me this 5th day of February, 2008



The Honorable Leonard P. Stark
United States Magistrate Judge